EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	297	("LAMBERT, ROBERT" or "GALLANT, ROBERT" or "MULLIN, RONALD" or "VANSTONE, SCOTT")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:19
L2	20	l1 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:55
L3	5	l2 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:55
L4	176	"CERTICOM CORP"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:55
L5	15	l4 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:00
L6	1	l5 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:58
L7	161	(("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 07:58
L8	17	l7 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:00
L9	4	l8 and (("finite" adj "field") with ((exchang$3 or chang$3 or swap$4) with (key$1 or "cryptographic key")))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:00
L10	1204	380/44	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:00
L11	14	l10 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:16

EAST Search History

L12	1	l11 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:18
L13	0	l11 and (("finite" adj "field") with ((exchang$3 or chang$3 or swap$4) with (key$1 or "cryptographic key")))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:01
L15	0	l11 and (("finite" adj "field") with ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:17
L16	1	l10 and (("finite" adj "field") with ((exchang$3 or chang$3 or swap$4) with (key$1 or "cryptographic key")))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:03
L19	229	380/285	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:13
L20	5	l19 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:33
L21	0	l19 and (("finite" adj "field") with ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:17
L22	16	l19 and (("finite" adj "field") and ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:34
L23	0	l22 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:34
L25	111	380/280	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:33
L26	0	l25 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:35
L27	1	l25 and (("finite" adj "field") and ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:35

EAST Search History

L28	1	l25 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:35
L29	695	713/171	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 08:34
L30	5	l29 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:28
L31	4	l30 and (("finite" adj "field") and ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:28
L32	0	l31 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:29
L33	180	708/204	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:28
L34	0	l33 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:30
L35	0	l33 and (("finite" adj "field") and ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:31
L36	0	l33 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:30
L37	19	708/206	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:29
L38	0	l37 and ("basis" adj "conversion")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:30
L39	21	708/442	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:30

EAST Search History

L40	1	l39 and (("finite" adj field$1) with cryptograph$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:30
L41	0	l40 and (("finite" adj "field") and ((key$1 or "cryptographic key") with (exchang$3 or chang$3 or swap$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:31
L42	6	708/809	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/03/17 10:31

Results for "((finite field and basis conversion)<in>metadata)"

e-mail printer friendly

Your search matched **3** of **1328352** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((finite field and basis conversion)<in>metadata) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **An efficient basis conversion algorithm for composite fields with given representations**
 Sunar, B.;
 Computers, IEEE Transactions on
 Volume 54, Issue 8, Aug. 2005 Page(s):992 - 997
 Digital Object Identifier 10.1109/TC.2005.124
 AbstractPlus | Full Text: PDF(128 KB) **IEEE JNL**
 Rights and Permissions

2. **VLSI structures for bit-serial modular multiplication using basis conversion**
 Parker, M.G.; Benaissa, M.;
 Computers and Digital Techniques, IEE Proceedings-
 Volume 141, Issue 6, Nov. 1994 Page(s):381 - 390
 AbstractPlus | Full Text: PDF(612 KB) **IEE JNL**

3. **Low complexity parallel multiplier in $F(q^n)$ over F_q**
 Huapeng Wu; Anwar Hasan, M.; Blake, I.F.;
 Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on [see also Circuits and Systems I: Regular Papers, IEEE Transactions on]
 Volume 49, Issue 7, July 2002 Page(s):1009 - 1013
 Digital Object Identifier 10.1109/TCSI.2002.800836
 AbstractPlus | References | Full Text: PDF(321 KB) **IEEE JNL**
 Rights and Permissions

© Copyright 2006 IEEE – All Rights Reserved

Indexed by Inspec

Results for "((cryptographic key exchange)<in>metadata)"

e-mail printer friendly

Your search matched **1** of **1328352** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((cryptographic key exchange)<in>metadata) Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items **Select All** **Deselect All**

☐ 1. **Methods and protocols for secure key negotiation using IKE**
Borella, M.S.;
Network, IEEE
Volume 14, Issue 4, July-Aug. 2000 Page(s):18 - 29
Digital Object Identifier 10.1109/65.855476
AbstractPlus | Full Text: PDF(1052 KB) **IEEE JNL**
Rights and Permissions

Indexed by Inspec

© Copyright 2006 IEEE – All Rights Reserved

Yahoo! My Yahoo! Mail Welcome, **Guest** [Sign In] Search Home Help

Web | Images | Video | Audio | Directory | Local | News | Shopping | More »

YAHOO! SEARCH finite field and basis conversion Search

My Web Answers BETA Search Services Advanced Search Preferences

Search Results Results **1 - 10** of about **409,000** for **finite field and basis conversion** - 0.18 sec. (About this page

1. Storage-Efficient **Finite Field Basis Conversion**
 Storage-Efficient **Finite Field Basis Conversion** Storage-Efficient **Finite Field Basis Conversion** . The problem of **finite field basis conversion** is to convert from the representation of a **field** element in one **basis** to the representation of the ...
 citeseer.ist.psu.edu/188239.html - More from this site - Save

2. RSA Security - Storage-efficient **finite field basis conversion**. SAC'98.
 Storage-efficient **finite field basis conversion**. SAC'98. Burton S. Kaliski Jr. **and** Yiqun Lisa Yin. Citation: B.S. Kaliski Jr. **and** Y.L. Yin. Storage-efficient **finite field basis conversion**. In S. Tavares **and** H. ... Abstract: The problem of **finite field basis conversion** is to convert from the representation of a **field** element ...
 www.rsasecurity.com/rsalabs/node.asp?id=2026 - 12k - Cached - More from this site - Save

3. **finite field basis conversion** methods (MICROSOFT POWERPOINT)
 ... RSA Data Security, Inc. **Finite Field Basis Conversion** Methods ... **Finite Field** Representation. A **basis** for the **finite field** GF(qm) over GF(q) is a set of elements □0, ..., □m-1 such ...
 rsasecurity.com/.../kaliski-yin-liskov-**basis-conversion**-pks-1999.ppt - 552k - View as html - More from this site - Save

4. http://www.wipo.int/cgi-pct/guest/getbykey5?KEY=00/52877.000908&ELEMENT_SET=DECL
 BACKGROUND OF THE INVENTION Cryptographic operations are generally implemented on elements in a **finite field**. ... METHOD **AND** APPARATUS FOR **FINITE FIELD BASIS CONVERSION** The present invention ... **conversion** of elements in a **finite field** having one **basis** to elements of a **finite field** having another ...
 wipo.int/cgi-pct/guest/getbykey5?KEY=00/52877.000908&ELEMENT_SET=DECL - 50k - Cached - More from this site - Save

5. Constructing Composite **Field** Representations for Efficient **Conversion**
 ... **and** M. Liskov, Efficient **Finite Field Basis Conversion** Involving Dual Bases Cryptographic ... Yin, Storage-Efficient **Finite Field Basis Conversion** Selected Areas in Cryptography ...
 csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/trans/tc/... - 22k - Cached - More from this site - Save

6. Microsoft Word - Document1 (PDF)
 Efficient **Finite Field Basis Conversion** Techniques. (Submission to IEEE P1363a) Burt Kaliski, Moses Liskov. 1. **and** Yiqun Lisa Yin. 2. RSA Laboratories. Abstract. This summary of **finite field basis conversion**

grouper.ieee.org/groups/1363/P1363a/contributions/**basis-conversion**.pdf - 26k - View as html - More from this site - Save

7. IEEE P1363a: Additional number-theoretic algorithms
IEEE P1363a: Additional number-theoretic algorithms. A new aspect of dual **basis** for efficient **field** arithmetic. Chang-Hyi Lee **and** Jong-In Lim, August 1998. ... This summary of **finite field basis conversion** techniques is proposed for inclusion in ... P1363a specifying storage-efficient **finite field basis conversion** techniques. Like IEEE P1363a ...
grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html - 10k - Cached - More from this site - Save

8. **Finite field** inverse circuit (US6009450)
... Abstract: A **finite field** inverse circuit has a **finite field** data unit (1112) **and** an inverse control unit (1110 ... Methods **and** apparatus for efficient **finite field basis conversion** ...
www.delphion.com/details?pn=US06009450__ - 62k - Cached - More from this site - Save

9. SEBC - Storage Efficient **Basis Conversion** for Elliptic Curve Cryptography (PDF)
... "Methods **and** Apparatus for Efficient **Finite Field Basis**. **Conversion**" enhances interoperability between **basis** sets ... the overhead required for adding **conversion**. capabilities to devices ...
www.firstprincipals.com/RSADataEncrypt.pdf - 29k - View as html - More from this site - Save

10. RSA Patent
United States Patent 5,854,759. Kaliski, Jr. , et al. December 29, 1998. Methods **and** apparatus for efficient **finite field basis conversion**. Abstract ... a first **basis** an element of a **finite field** GF(q.sup.m ...
www-scf.usc.edu/~bilalsha/RSAPatent.htm - 3k - Cached - More from this site - Save

Results Page:
1 2 3 4 5 6 7 8 9 10 **Next**

Web | Images | Video | Audio | Directory | Local | News | Shopping | More »
Your Search: finite field and basis conversion Search

Didn't find what you needed? Try Yahoo! Answers.

Copyright © 2006 Yahoo! Inc. All rights reserved. Privacy Policy - Terms of Service - Copyright/IP Policy - Submit Your Site

Yahoo! My Yahoo! Mail Welcome, **Guest** [Sign In] Search Home Help

Web | Images | Video | Audio | Directory | Local | News | Shopping | More »

YAHOO! SEARCH cryptographic operations and basis conversion Search

My Web Answers BETA Search Services Advanced Search Preferences

Search Results Results **1 - 10** of about **80,100** for **cryptographic operations and basis conversion** - 0.19 sec. (A

1. http://www.wipo.int/cgi-pct/guest/getbykey5?KEY=00/52877.000908&ELEMENT_SET=DECL
BACKGROUND OF THE INVENTION **Cryptographic operations** are generally implemented on elements in a finite field. ... **AND** APPARATUS FOR FINITE FIELD **BASIS CONVERSION** The present invention relates to **cryptographic** systems **and** ... **and** B perform **cryptographic operations** n a **basis**, ßI **and**/%, respectively ...
wipo.int/cgi-pct/guest/getbykey5?KEY=00/52877.000908&ELEMENT_SET=DECL - 50k - Cached - More from this site - Save

2. 1 Introduction (PDF)
... systems, particularly for **cryptographic operations**. Among the more common ... **operations** in either **basis**. Thus, the **conversion** process may not be as e cient ...
grouper.ieee.org/groups/1363/Research/contributions/**basis**conv.pdf - 194k - View as html - More from this site - Save

3. Constructing Composite Field Representations for Efficient **Conversion**
... Efficient Finite Field **Basis Conversion** Involving Dual Bases **Cryptographic** Hardware **and** Embedded Systems ... A Fast Software Implementation for Arithmetic **Operations** in GF(2^n)," Proc ...
csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/trans/tc/... - 22k - Cached - More from this site - Save

4. Storage-Efficient Finite Field **Basis Conversion**
Storage-Efficient Finite Field **Basis Conversion** Storage-Efficient Finite Field **Basis Conversion** . The problem of finite field **basis conversion** is to convert from the representation of a field element in one **basis** to the representation of the ...
citeseer.ist.psu.edu/188239.html - More from this site - Save

5. Elliptic Curve Cryptography
SEBC - Storage Efficient **Basis Conversion**. for Elliptic Curve Cryptography. OPPORTUNITY. RSA Security Inc. ... than other **cryptographic** methods to achieve ... **basis conversion** approaches. Provide greater computational efficiency in that they involve primary or exclusive finite field **operations** ...
www.iptrade.net/ecc.html - 6k - Cached - More from this site - Save

6. SEBC - Storage Efficient **Basis Conversion** for Elliptic Curve Cryptography (PDF)
... SEBC - Storage Efficient **Basis Conversion** ... size than other. **cryptographic** methods to achieve equivalent security ... primary or exclusive finite field **operations**. rather than more complex ...
www.firstprincipals.com/RSADataEncrypt.pdf - 29k - View as html - More from this site - Save

Results Page:

1 2 3 4 5 6 7 8 9 10 Next

7. http://www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/**basis-conversion**/kaliski-yin-bas... (MICROSOFT POWERPOINT)
... Storage-Efficient Finite Field **Basis Conversion**. Burt Kaliski **and** Yiqun ... intermediate values in **cryptographic** primitives, such as DSA ... Wm-1 with internal **basis operations**. Accumulate B[i ...
rsasecurity.com/rsalabs/.../kaliski-yin-**basis-conversion**-sac-1998.ppt - 146k - View as html - More from this site - Save

8. S/390 Parallel Enterprise Server CMOS **Cryptographic** Coprocessor
... Internet becomes the **basis** for electronic commerce, **and** ... perform PIN **operations**, **and** perform other **cryptographic** functions dealing ... modulo multiplier, **and** some **conversion and** cleanup ...
www.research.ibm.com/journal/rd/435/easter.html - 74k - Cached - More from this site - Save

9. finite field **basis conversion** methods (MICROSOFT POWERPOINT)
... Finite Field **Basis Conversion** Methods. Burt Kaliski ... intermediate values in **cryptographic** primitives, such as DSA ... cases, ideally with field **operations** in the internal representation ...
rsasecurity.com/.../kaliski-yin-liskov-**basis-conversion**-pks-1999.ppt - 552k - View as html - More from this site - Save

10. Constructing Composite Field Representations for Efficient **Conversion** (PDF)
... We derive the **conversion** (change of **basis**) matrix. The special case of when ... for implementing the finite field arithmetic. **operations** particularly for **cryptographic** applications [13 ...
islab.oregonstate.edu/papers/j59comf.pdf - 142k - View as html - More from this site - Save

Web | Images | Video | Audio | Directory | Local | News | Shopping | More »
Your Search: cryptographic operations and basis conversion Search

Didn't find what you needed? Try Yahoo! Answers.

Copyright © 2006 Yahoo! Inc. All rights reserved. Privacy Policy - Terms of Service - Copyright/IP Policy - Submit Your Site